

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
INSTAGRAM ACCOUNT “mrksl24” THAT
IS STORED AT PREMISES CONTROLLED
BY META PLATFORMS, INC.

No. 2:25-mj-00204-KFW

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Douglas Foster, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), an electronic communications service and/or remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Internal Revenue Service – Criminal Investigation (IRS-CI) and have been since December 12, 2023. I am currently assigned to the IRS-CI in South Portland, Maine. From June 6, 2023 to December 12, 2023 I was a Special Agent in Training at the Federal Law Enforcement Training Center in Glynco, Georgia where I graduated

from both the Criminal Investigator Training Program (CITP) and the Special Agent Basic Training (SABT) program. During the six-month training program, I was trained on many subjects ranging from general law enforcement trainings to specific tax and money laundering violations. These trainings included courses, exams, and practical exercises on digital evidence, search warrants as investigative tools, and violations under the purview of IRS-CI including Title 18 of the United States Code.

3. I am familiar with the facts and circumstances of this investigation, and I have received information from a variety of sources, including but not limited to other law enforcement officers, subpoenaed records, governmental records, and internal IRS records. In addition, I have reviewed records and reports relating to this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S. Code §§ 371 (Conspiracy to Commit Offense or to Defraud the United States), 472 (Counterfeit Obligations), 1344 (Bank Fraud), and 514 (Fictitious Obligations) have been committed by Keith Mitchell and other co-conspirators. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Based upon my training and experience, the training and experience of my on-the-job instructor, and conversations with other law enforcement officers, and knowledge of other investigations, I am aware that a scheme exists to obtain and use the information from valid United States Treasury checks in order to fraudulently obtain funds originally issued as tax refunds. The scheme involves stealing or otherwise obtaining the information from a valid U.S. Treasury check and subsequently creating and printing a fraudulent check intended to be deposited and passed off as a valid check. This fraudulently created check will bear the name of the person who will deposit the check into a financial institution, but also contains the amount, symbol number, and serial number from a valid U.S. Treasury check.

7. While there are many different ways the scheme can be conducted, it is common for the checks to be sold online, in which case the buyer will receive the check with their name and address on it and deposit the check. For the period involved in this case, between April 15, 2024, and June 26, 2024, the main tool for financial institutions to check the validity of a U.S. Treasury check was the Treasury Check Verification System (TCVS). The TCVS compares the amount, symbol number, and serial number against valid U.S. Treasury checks. If all three match the TCVS returns that the check is valid. Unless the bank makes further attempts to confirm the validity of the check, for example inspecting the security features (watermark, microprinting, etc.), or receives a check reclamation form from the U.S. Treasury, the check will be accepted as valid and the depositor will gain access to the funds. Therefore, even with an altered name and address, the perpetrators of this scheme would be able to deposit fraudulent treasury checks so long as they obtained and used the amount, symbol number, and serial number from a valid U.S. Treasury Check.

8. On June 28, 2024, IRS-CI agents Joseph Durak and I received a report from the Saco Police Department regarding Keith Mitchell. Saco and Biddeford Savings Institution, a regional bank with multiple locations in Southern Maine, filed a police report about fraudulent U.S. Treasury checks deposited into the account of Keith Mitchell. In total, thirteen (13) U.S. Treasury checks totaling \$83,632.09 were deposited into Keith Mitchell's account across three (3) different branches between April 15 and June 20, 2024. Eight (8) of the deposited checks were obtained by the Saco Police Department as evidence. The other five (5) checks deposited had already been destroyed per bank policy.

| Symbol | Serial Number | Date Deposited | Amount | Location Deposited | Alleged Depositor | Current Status |
|--------|---------------|----------------|-------------|--------------------|-------------------|-------------------|
| 4045 | 32228478 | 4/15/2024 | \$5,576.00 | Scarborough, ME | Mitchell | Destroyed |
| 4045 | 43284717 | 4/19/2024 | \$4,404.00 | South Portland, ME | Sands | Destroyed |
| 4045 | 42975764 | 4/24/2024 | \$8,846.00 | Saco, ME | Sands | Destroyed |
| 4045 | 42975771 | 4/26/2024 | \$6,963.00 | South Portland, ME | Sands | Destroyed |
| 4045 | 42975765 | 4/30/2024 | \$7,756.00 | Westbrook, ME | Sands | Destroyed |
| 4045 | 46090385 | 5/3/2024 | \$2,600.00 | Westbrook, ME | Sands | IRS-CI Possession |
| 4045 | 42975839 | 5/3/2024 | \$2,359.00 | Westbrook, ME | Sands | IRS-CI Possession |
| 4045 | 42524227 | 5/3/2024 | \$1,435.22 | Westbrook, ME | Sands | IRS-CI Possession |
| 4045 | 48250314 | 5/9/2024 | \$9,527.87 | South Portland, ME | Mitchell | IRS-CI Possession |
| 4045 | 42968856 | 5/9/2024 | \$2,383.00 | South Portland, ME | Mitchell | IRS-CI Possession |
| 4045 | 48273276 | 5/16/2024 | \$10,983.00 | Scarborough, ME | Mitchell | IRS-CI Possession |
| 4045 | 50346784 | 6/5/2024 | \$11,196.00 | South Portland, ME | Sands | IRS-CI Possession |
| 4045 | 50381438 | 6/20/2024 | \$9,423.00 | South Portland, ME | Mitchell | IRS-CI Possession |

9. Detective Ryan Hatch of the Saco Police Department reviewed ATM camera footage from April 15 and May 16, 2024, and stated that the person “does closely match the description of Keith Mitchell who I am familiar with from a previous police investigation.”

10. On July 16, 2024, I took custody of the eight (8) treasury checks obtained by Saco PD. The checks were submitted to the Center for Science and Design (CSD) to be analyzed and

fingerprinted. On October 15, 2024, a report was issued by the CSD stating that each U.S. Treasury check deposited into Keith Mitchell's account contained inconsistencies relating to eight (8) different security features present on a standard U.S. Treasury check reference, including lack of watermark and lack of microprinting. On December 9, 2024, a report was issued by the CSD identifying the fingerprints of Michael Reid (FBI#: 287145KD1) on four (4) of the checks examined by fingerprint specialist Peggy Konrath.

11. Pursuant to an order obtained on April 16, 2025, under IRC 6103(i), Department of Treasury, Internal Revenue Service records were received regarding the U.S. Treasury checks bearing the symbol number, serial number, and amounts matching the checks deposited into Keith Mitchell's account. The records show the official checks were issued to other individuals, with names and addresses not matching that of Keith Mitchell.

12. Pursuant to the same order discussed above, obtained on April 16, 2025, IRS records show tax returns filed by Keith Mitchell show refunds due to Mitchell for his 2021, 2022, and 2023 tax returns. These refunds do not match any amount of any check deposited, and each of the refunds for Mitchell were elected to be paid via direct deposit on each of Mitchell's Forms 1040.

13. On September 12, 2024, I received records from Saco and Biddeford Savings Institution pursuant to a subpoena issued by the U.S. Attorney's Office. The records included surveillance video which shows Keith Mitchell depositing checks at the Saco and Biddeford Savings Institution, Scarborough Branch, on April 15, 2024, and May 16, 2024. The videos also show a white female driving a white Chevrolet sedan, Maine License plate "627 ADV" depositing some of the fraudulent checks into Keith Mitchell's account at the Westbrook Branch on April 30, 2024, and May 3, 2024, as well as the Saco Branch on April 24, 2024. Through

DMV registration records and a driver's license photo, the white female was identified as Michelle Sands of Brewer, Maine.

14. On November 7, 2024, Brewer Police Department Sergeant Zachary Caron provided IRS-CI a police report of Michelle Sands depositing a U.S. Treasury Check into her Bangor Federal Credit Union account that was returned for unauthorized negotiation. Records subpoenaed from Bangor Federal Credit Union show Michelle Sands deposited five (5) U.S. Treasury Checks totaling \$23, 675.84 between May 16, 2024, and June 26, 2024, suspected to be fraudulent. The checks were submitted to the CSD to be analyzed and fingerprinted. On February 4, 2025, a report was issued by the CSD stating that each U.S. Treasury check deposited into Michelle Sands' account contained inconsistencies relating to eight (8) different security features present on a standard U.S. Treasury check reference, including lack of watermark and lack of microprinting. No fingerprints suitable for identification were preserved on the checks.

15. Pursuant to an order obtained on April 16, 2025, under IRC 6103(i), Department of Treasury, Internal Revenue Service records were received regarding the U.S. Treasury checks bearing the symbol number, serial number, and amounts matching the checks deposited into Michelle Sands' account. The records show the official checks were issued to other individuals, with names and addresses not matching that of Michelle Sands.

16. Pursuant to the same order discussed above, obtained on April 16, 2025, IRS records show tax returns filed by Michelle Sands show refunds due to Sands for her 2021, 2022, and 2023 tax returns. These refunds do not match any amount of any check deposited, and each of the refunds for Sands were elected to be paid via direct deposit on each of Sand's Forms 1040.

17. On January 17, 2025, I interviewed Michelle Sands. During the interview she stated that she deposited some checks on behalf of her boyfriend, Keith Mitchell, into his Saco

and Biddeford Savings Institution account. Sands said that she did not know what the checks were for or where Mitchell got them. Sands stated she believed the five (5) U.S. Treasury Checks she deposited into her Bangor Federal Credit Union account were for her tax refund.

18. On February 3, 2025, I interviewed Keith Mitchell. During the interview Mitchell stated that he communicated with and was “scammed” by someone on Instagram named “Mr. Stimulus”. Mitchell claimed to have given his bank account login information, Cash App login information, name, address, and social security number to “Mr. Stimulus”. Mitchell said that he received the checks in the mail and deposited some of the checks himself and asked Michelle Sands to deposit some of the checks for him. Mitchell said that “Mr. Stimulus” has since blocked him on Instagram and he could not see their old messages.

19. Throughout the investigation I have reviewed records subpoenaed from Block, Inc. detailing Cash App transactions made by the accounts of Keith Mitchell, Michelle Sands, and Michael Reid as well as Green Dot Corporation records detailing Apple Pay transactions made by Keith Mitchell and Michael Reid. The Apple Pay records show Michael Reid registered with an email account of mike.bo1468@icloud.com and the Cash App records show Michael Reid registered three (3) separate Cash App accounts using Cashtags (unique identifiers for individuals using Cash App) of “srtmikebo”, “mikebo1468”, and “mikebo152”.

20. Research of Michael Reid’s criminal history show he is on probation until March 21, 2029. Reid has a federal conviction for attempt and conspiracy to commit fraud as well as state convictions for possession of a forged instrument and murder in the second degree. His current residence is 152 Marcus Garvey Blvd, Apt 3G, Brooklyn, NY. Mitchell denied knowing Michael Reid, but both Reid and Mitchell served time at Ray Brook Federal Correctional Institute during the overlapping period from April 6, 2023 until March, 18, 2024.

21. Apple Pay records show Keith Mitchell sent Michael Reid a total of \$16,400.00 between April 16, 2024 and June 24, 2024. Cash App Records show Keith Mitchell sent Asia Mathison \$18,349.00 between April 20, 2024 and May 17, 2024. Asia Mathison sent \$6,334.00 either directly to Michael Reid, or to other Cash App accounts with a note added “for Mike Bo”, “Mikey Bo”, Mike”, or “Bo”.

22. Following my interview of Mitchell, and based on his claim that he communicated with a “Mr. Stimulus” via Instagram, the U.S. Attorney’s Office requested an order pursuant to 18 U.S.C. § 2703(d) for records related to Instagram accounts belonging to Mitchell, including account @mrksl24. On March 3, 2025, Magistrate Judge Karen Wolf issued the requested order.¹ I received and reviewed Instagram records provided to the U.S. Attorney’s Office pursuant to the order. In the records I noted the following:

- a. The “Mrksl24” Instagram account has a verified email address of kslda1@icould.com. Subpoenaed records from Block, Inc. show Keith Mitchell registered for Cash App using the email kslda1@icloud.com. Additional records obtained from Blue Acorn show Keith Mitchell applied for a Paycheck Protection Program (PPP) Loan using the email kslda1@icloud.com.
- b. I was unable to find messages with anyone named “Mr. Stimulus” and I performed searches for similar names and possible alternate spellings but was not able to locate any results.
- c. The “Mrksl24” account was deactivated on February 4, 2025, only one day after Agent Durak and I interviewed Mitchell about the fraudulent checks.

¹ Case No. 2:25-mj-00110-KFW.

- d. “Mrksl24” exchanged approximately 100 messages with “srt_mikebo” between March 27, 2024, and January 5, 2025. Kieth Mitchell stated during our interview that he did not know anyone named Michael Reid or anyone who went by the nickname of Mikey Bo.
 - e. “Mrksl24” exchanged approximately 70 messages with “shellz886”, with a display name “Michelle Sands” starting on April 15, 2024, and ending January 16, 2025.
23. A preservation request related to the @mrksl24 Instagram account was sent on March 18, 2025, via Meta’s online law enforcement portal. Case number 9372637 was assigned by Meta and confirmation was received via email.

BACKGROUND CONCERNING INSTAGRAM²

24. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

² The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: “Privacy Policy,” <https://privacycenter.instagram.com/policy/>; “Information for Law Enforcement,” <https://help.instagram.com/494561080557017>; and “Help Center,” <https://help.instagram.com>.

25. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

26. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

27. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

28. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

29. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

30. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

31. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography (“Bio”), and a website address.

32. One of Instagram’s primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users (“tag”), or add a location. These appear as posts on the user’s profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta’s servers.

33. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can “mention” others by adding their username to a comment followed by “@”). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

34. An Instagram “story” is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain on Meta’s servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

35. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram’s long-form video app.

36. Instagram Direct, Instagram’s messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with “disappearing” photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can’t view their disappearing messages after they are sent but do have access to each message’s status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

37. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

38. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be “followed” to generate related updates from Instagram. Meta retains records of a user’s search history and followed hashtags.

39. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

40. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user’s identity and activities, and it can also reveal potential sources of additional evidence.

41. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support

services, as well as records of any actions taken by the provider or user as a result of the communications.

42. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

43. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, 18 U.S. Code § 371 requires an agreement by two or more parties; evidence obtained from direct messages on Instagram may show the existence or lack of existence of such an agreement.

44. The stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Records already provided by Meta pursuant to a 2703(d) order filed on March 3, 2025, show communications between subjects of the criminal investigation around the time the criminal actions were being committed. Statements made by the subject to investigators assert that Instagram messaging was the sole method of communication between the subject and the source of the fraudulent checks. Based on my training and experience, instant messages, photos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

45. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. This information is relevant to establish jurisdiction for communications that could prove 18 U.S. Code § 371, conspiracy to defraud United States, as well as ascertain the degree of truth supporting statements made by the subject to investigators.

46. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

47. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, stored communications, contact lists, photos, and videos can

lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

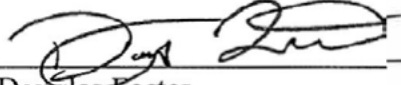
48. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant.

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



Respectfully submitted,

 6/5/2025
Douglas Foster
Special Agent
IRS – Criminal Investigation

Sworn to telephonically and signed
electronically in accordance with the
requirements of Rule 4.1 of the Federal Rules
of Criminal Procedures

Date: Jun 05 2025

City and state: Portland, Maine


Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title